

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11215122 A**

(43) Date of publication of application: **06.08.99**

(51) Int. Cl.

H04L 9/36
G09C 1/00

(21) Application number: **10013727**

(22) Date of filing: **27.01.98**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD.**

(72) Inventor: **HARADA TOSHIHARU**
OKUMURA YASUO
TATEBAYASHI MAKOTO
SAIJO TAKESHI
ONO TAKATOSHI

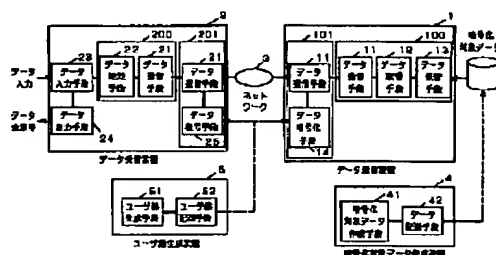
**(54) METHOD, DEVICE, AND SYSTEM FOR
ENCIPHERING DATA**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method, device, and system for enciphering data by which only the necessary scope of data distributed through WWW(world-wide web) can be enciphered in accordance with the contents of the data.

SOLUTION: (1) A data receiver 2 transmits data request information and receiver identification information when a user inputs data required by the user in a WWW browser 200. (2) A data transmitter 1 enciphers the data to be enciphered corresponding to the data requesting information and incorporating an enciphering scope designating instruction within the extent designated by the enciphering scope designating instruction in such a way that only the receiver can decode the enciphered data in an enciphering proxy 101 and transmits the results to the data receiver 2. (3) The data receiver 2 decodes the enciphered data in a decoding proxy 201 and outputs the decoded data.

COPYRIGHT: (C)1999,JPO



(10) 日本国特許庁 (P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-215122

(43) 公開日 平成11年(1999) 8月6日

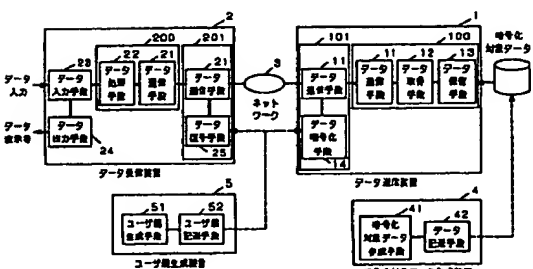
(51) Int. Cl. ⁴	国際記号	P 1	H 04 L 9/38 G 09 C 1/00	6 8 5 6 6 0 2
(21) 出願番号	特願平10-13727	(71) 出願人	00005821 松下電器産業株式会社	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(22) 出願日	平成10年(1998) 1月27日	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(71) 出願人	00005821 松下電器産業株式会社	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治
(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者	大坂府門真市大字門真1006番地 松下電器 豊田 健治	(72) 発明者 大坂府門真市大字門真1006番地 松下電器 豊田 健治

(54) 発明の名称 データ暗号方法、データ暗号装置、及びデータ暗号システム

(57) [要約]

【課題】 暗号で暗号化されるデータに対して、その内容に応じて必要な範囲だけを暗号化する方法、装置及びシステムを提供する。

【解決手段】 (1) データ受信装置 2 は、暗号プロセッサ 200 において、ユーザから取得したいデータの受け取りを受け、データ要求情報と受信者識別情報を送信する。(2) データ送信装置 1 は、暗号プロセッサ 101 において、データ要求情報に付随した、暗号化範囲指定命令が組み込まれた暗号化対象データに対して、暗号化範囲指定命令で指定された範囲を、受信者識別情報で指定された受信者のみが復号できるように暗号化し、この結果をデータ受信装置 2 に送信する。(3) データ受信装置 2 は、復号プロセッサ 201 において暗号化された暗号化対象データを復号し、復号されたデータを取り出す。



【特許請求の範囲】

【請求項 1】 暗号化処理方法を含むデータ処理方法に指定する命令が組み込まれた暗号化対象データに対して、組み込まれた命令に従って暗号化処理を含むデータ処理を行うデータ暗号方法であって、

暗号化する範囲を指定する暗号化範囲指定命令が組み込まれた暗号化対象データに対して、前記暗号化範囲指定命令で指定された範囲を暗号化することを特徴とするデータ暗号方法。

【請求項 2】 前記暗号化対象データに、前記暗号化範囲指定命令に加えて、前記暗号化対象データの受信者を指定する受信者指定命令が組み込まれている場合に、前記受信者指定命令で指定された受信者が保持する復号鍵に対応する暗号化鍵を用いて、前記暗号化対象データの暗号化を行うようにしたことを特徴とする請求項 1 記載のデータ暗号方法。

【請求項 3】 前記暗号化対象データを暗号化するには、前記暗号化対象データを第 1 の暗号化鍵で暗号化し、前記第 1 の暗号化鍵に付随する第 1 の復号鍵を、受信者の保持する第 2 の復号鍵に付随する第 2 の暗号化鍵で暗号化し、暗号化された前記暗号化対象データに、暗号化された前記第 1 の復号鍵を指定する暗号化範囲指定命令を組み込んだ暗号化データを得るようになことを特徴とする請求項 1 記載のデータ暗号方法。

【請求項 4】 復号処理方法を含むデータ処理方法に指定する命令が組み込まれた暗号化データに対して、組み込まれた命令に従って復号処理を含むデータ処理を行うデータ暗号方法であって、

復号する範囲を指定する復号範囲指定命令が組み込まれた暗号化データに対して、前記復号範囲指定命令で指定された範囲を復号することを特徴とするデータ暗号方法。

【請求項 5】 前記暗号化データに、前記復号範囲指定命令に加えて、暗号化データの受信者を指定する受信者指定命令が組み込まれている場合に、

前記受信者指定命令で指定された受信者が保持する復号鍵を用いて、前記暗号化データに対して、前記復号範囲指定命令により指定された範囲を前記復号鍵を用いて復号するようにしたことを特徴とする請求項 4 記載のデータ暗号方法。

【請求項 6】 前記暗号化データに、前記復号範囲指定命令に加えて、暗号化された前記第 1 の復号鍵を指定する暗号化範囲指定命令が組み込まれている場合に、

前記暗号化データに、前記第 1 の復号鍵を指定する暗号化範囲指定命令に付随する暗号化範囲指定命令で指定された範囲を前記第 1 の復号鍵を用いて復号するようにしたことを特徴とする請求項 6 記載のデータ暗号方法。

4 記載のデータ暗号方法。

【請求項 7】 前記暗号化対象データに組み込まれる命令が、特に、HTML (Hypertext Markup Language) 言語に基いた命令である場合に、暗号化処理のための命令部、すなわち前記暗号化範囲指定命令、前記復号範囲指定命令、前記受信者指定命令、及び、前記復号範囲指定命令の記述方法として、前記HTMLで定義されているコメント指定用の命令を利用し、そのコメントとしてあらかじめ定められた特定のコメントが指定された時に前述の暗号化処理のための命令部の中から対応する命令が指定されたものとみなすようにしたことを特徴とする請求項 1 から 6 のうちのいずれか 1 項記載のデータ暗号方法。

【請求項 8】 暗号化処理方法を含むデータ処理方法に指定する命令が組み込まれた暗号化対象データに対して、組み込まれた命令に従って暗号化処理を含むデータ処理を行うデータ暗号方法であって、データ暗号化手段と、データ復号手段と、データ保管手段と、データ暗号化手段とを備え、

前記データ暗号化手段が、前記データ保管手段に保管された暗号化対象データの暗号化を要求するデータ要求情報を送信し、前記データ復号手段が、前記データ要求情報で要求された前記暗号化対象データを前記データ保管手段から取得し、前記データ暗号化手段が、前記暗号化手段から取得した前記暗号化範囲指定命令により指定された範囲を暗号化し、この結果として得られる少なくとも一部が暗号化された前記暗号化対象データに、復号する範囲を指定する復号範囲指定命令を組み込んだ暗号化データを生成し、データ暗号化手段が、前記暗号化データを前記データ要求情報の発信元に送信することを特徴とするデータ暗号装置。

【請求項 9】 前記データ暗号化手段が、特に、前記データ暗号化手段と、前記データ復号手段と、前記データ保管手段とを備えた暗号化装置 (World Wide Web) と、前記データ暗号化手段とを有する暗号化プログラムとが実行されたコンピュータであることとを特徴とする請求項 8 記載のデータ暗号装置。

【請求項 10】 前記暗号化プログラムが、前記データ暗号化手段に加えて、暗号化データまたは暗号化データと、前記暗号化対象データもしくは前記暗号化データの送受信を行うためのデータ暗号化手段とを有するプログラムであることを特徴とする請求項 9 記載のデータ暗号装置。

【請求項 11】 復号処理方法を含むデータ処理方法に指定する命令が組み込まれた暗号化データに対して、組み込まれた命令に従って復号処理を含むデータ処理を行うデータ暗号方法であって、データ暗号化手段と、データ復号手段と、データ入力手段と、データ出力手段と、データ暗号化手段とを備え、

前記データ入力手段に、外部から取得したい暗号化対象データを指定する暗号化入力されたとき、前記データ暗号化手段が、前記暗号化対象データの暗号化を要求するデータ

ヲ要求情報を送信し、前記データ要求情報に対応する、復号する範囲を指定する復号範囲指定命令を組み込まれた暗号化データを受信し、前記データ復号手段が、前記暗号化データのうち復号範囲指定命令で指定された範囲を復号し、前記データ復号手段が、復号された暗号化データを、デイスクリプタリソングなどのデータ出力装置が接続された前記データ出力手段に出力することを特徴とするデータ暗号装置。

【請求項12】 前記データ受信装置が、特に、前記データ通信手段と、前記データ処理手段と、前記データ入力手段と、前記データ出力手段を備えたデータ装置と、前記データ復号手段を有する復号プログラムが接続されたコンピュータであることと特徴とする請求項1記載のデータ暗号装置。

【請求項13】 前記復号プログラムが、前記データ復号手段に加えて、暗号サーバまたは暗号クライアント、前記暗号化対象データもしくは前記暗号化データの送受信を行うためのデータ通信手段を有するプログラムであることを特徴とする請求項12記載のデータ暗号装置。

【請求項14】 データ通信手段と、データ取得手段と、データ保管手段と、データ暗号化手段と、ユーザ復号手段とを備えた送信側のデータ暗号装置と、データ通信手段と、データ処理手段と、データ入力手段と、データ出力手段と、データ復号手段と、ユーザ復号手段とを備えた受信側のデータ暗号装置と、ネットワークと、暗号化対象データ作成手段と暗号化対象データ配送手段を備えた暗号化対象データ作成装置と、ユーザ復号手段とユーザ配送手段を備えたユーザ復号生成装置とで構成されるデータ暗号システムであって、前記ユーザ復号生成装置において、前記ユーザ復号生成手段が、各ユーザ固有の暗号化鍵とこの暗号化鍵に対応する復号鍵を生成し、前記ユーザ配送手段が、前記暗号化鍵を前記送信側のデータ暗号装置のユーザ復号手段に保管し、前記復号鍵を前記受信側のデータ暗号装置のユーザ復号手段に保管し、

前記暗号化対象データ作成装置において、前記暗号化対象データ作成手段が、暗号化する範囲を指定する暗号化範囲指定命令を組み込んだ暗号化対象データを作成し、前記暗号化対象データ配送手段が、前記暗号化対象データを前記送信側のデータ暗号装置のデータ保管手段に保管し、

前記受信側のデータ暗号装置において、前記データ入力手段に、外部から取得したい暗号化対象データを指定する情報が入力されたとき、前記データ通信手段が、前記暗号化対象データの送受信を要求するデータ要求情報を前記送信側のデータ暗号装置に前記ネットワークを利用して送信し、

前記送信側のデータ暗号装置において、前記データ通信手段が、前記データ保管手段に保管された暗号化対象データの送受信を要求するデータ要求情報を受信したとき、

前記データ取得手段が、前記データ要求情報で要求された前記暗号化対象データを前記データ保管手段から取得し、前記データ暗号化手段が、前記暗号化対象データのうち前記暗号化範囲指定命令により指定された範囲を暗号化し、この結果として得られる少なくとも一部が暗号化された前記暗号化対象データに、復号する範囲を指定する復号範囲指定命令を組み込んだ暗号化データを作成し、データ通信手段が、前記暗号化データを前記受信側のデータ暗号装置に前記ネットワークを利用して送信し、

前記受信側のデータ暗号装置において、前記暗号化データを受信し、前記データ復号手段が、前記暗号化データのうちの復号範囲指定命令で指定された範囲を復号し、前記データ処理手段が、復号された暗号化データを、デイスクリプタリソングなどのデータ出力装置が接続された前記データ出力手段に出力することを特徴とするデータ暗号システム。

【請求項15】 データ通信手段と、データ取得手段と、データ保管手段とを備えた送信側のデータ暗号装置と、データ通信手段と、データ処理手段と、データ入力手段と、データ出力手段と、データ復号手段と、ユーザ復号手段とを備えた受信側のデータ暗号装置と、ネットワークと、暗号化対象データ作成手段と、データ暗号化手段と、ユーザ復号手段と、暗号化データ配送手段を備えた暗号化データ作成装置と、

ユーザ復号生成手段とユーザ配送手段を備えたユーザ復号生成装置とで構成されるデータ暗号システムであって、前記ユーザ復号生成装置において、前記ユーザ復号生成手段が、各ユーザ固有の暗号化鍵とこの暗号化鍵に対応する復号鍵を生成し、前記ユーザ配送手段が、前記暗号化鍵を前記暗号化データ作成装置のユーザ復号手段に保管し、前記復号鍵を前記受信側のデータ暗号装置のユーザ復号手段に保管し、

前記暗号化データ作成装置において、前記暗号化データ作成手段が、暗号化する範囲を指定する暗号化範囲指定命令を組み込んだ暗号化対象データを作成し、前記データ暗号化手段が、前記暗号化対象データのうち前記暗号化範囲指定命令により指定された範囲を暗号化し、この結果として得られる少なくとも一部が暗号化された前記暗号化対象データに、復号する範囲を指定する復号範囲指定命令を組み込んだ暗号化データを作成し、前記暗号化データ配送手段が、前記暗号化データを前記送信側のデータ暗号装置のデータ保管手段に保管し、

前記受信側のデータ暗号装置において、前記データ入力手段に、外部から取得したい暗号化対象データを指定する情報が入力されたとき、前記データ通信手段が、前記暗号化データの送受信を要求するデータ要求情報を前記送信側のデータ暗号装置に前記ネットワークを利用して送

信し、

前記送信側のデータ暗号装置において、前記データ通信手段が、前記データ保管手段に保管された暗号化データの送受信を要求するデータ要求情報を受信したとき、前記データ取得手段が、前記データ要求情報で要求された前記暗号化データを前記データ保管手段から取得し、データ通信手段が、前記暗号化データを前記受信側のデータ暗号装置に前記ネットワークを利用して送信し、

前記受信側のデータ暗号装置において、前記暗号化データを受信し、前記データ復号手段が、前記暗号化データのうちの復号範囲指定命令で指定された範囲を復号し、前記データ処理手段が、復号された暗号化データを、デイスクリプタリソングなどのデータ出力装置が接続された前記データ出力手段に出力することを特徴とするデータ暗号システム。

【発明の詳細な説明】

【発明の属する技術分野】 暗号処理命令を含むデータ処理命令の組み込まれた暗号化対象データに対して、組み込まれた命令に従って暗号処理を施すための方法、装置、及びシステムに関する。

【0002】

【従来の技術】 WWW(World Wide Web)システムは、ウェブブラウザの検索や、不特定多数への情報発信といった機能を、非常に簡便なユーザインタフェースで提供するため急速に普及している。このため、WWWシステムを、パソコンソフトのオンライン販売と、商用システムを構築する際のプラットフォームとして利用されている。

【0003】 WWWシステムを利用して発信される有料の電子情報や、郵便物の電子情報（以下、単に「データ」と称する）を、特定の受信者以外に送信（送信、送達）されたいようにするために、データ暗号化することが考えられる。また、特に商用利用の場合は、データ暗号化を、その内容に応じて、一部を視聴可能とし、重要な部分だけを暗号化するという、きめ細かく暗号化することが考えられる。

【0004】 従来、WWWシステムで発信する電子情報を暗号化する方法としては、NetscapeCommunications社が提供するSSL(Secure Socket Layer)や Enterprise Information Technologies社が提供するS-HTTPがあり、これらを用いるとWWWデータは暗号化されるため第三者への送信（送信）を防止することができ、なお、SSL及びS-HTTPについては、例えば、OJ出版社のOPEN DESIGN, 1996年6月号（第7巻）を参照されたい。

【0005】

【発明が解決しようとする課題】 しかしながら、これらの従来の方法は、いずれも、WWWデータを発信するサーバと、WWWデータを受信するクライアント間で伝送されるWWWデータ全体に対して一律的に暗号化するのであ

た。このため、データの内容に応じて、一部はすべての受信者に送信を可能とし、重要な部分だけを暗号化するという、きめ細かく暗号化が行えなかった。また、従来の方法では、上述のSSLまたはS-HTTPに基づく暗号機能が追加された利用のWWWサーバ及びWWWクライアントが必要であった。そして、例えば、SSLに基づく暗号機能が追加されたWWWサーバは、SSLに基づく暗号機能が追加されたWWWクライアントの両方のみ、WWWデータの暗号通信が可能であった。

【0006】 本発明は、上記従来の問題点に鑑み、WWWデータを暗号化するに際し、データの内部に応じて、必要な範囲だけを暗号化でき、また、必要であればあらかじめ指定した受信者のみが復号できるようにデータ暗号化を暗号化することも可能とする。データ暗号化方法、装置及びシステムを提供することを第1の目的とする。

【0007】

また、既存のWWWサーバやWWWクライアントに暗号機能を追加する必要のない、すなわち、本発明のデータ暗号化方法に基づく暗号機能が追加された利用のWWWサーバやWWWクライアントを必要としない、データの暗号化方法、装置、暗号化方法、装置及びシステムを提供することを第2の目的とする。

【0008】

【課題を解決するための手段】 上記目的を達成するために、本発明は、暗号化処理方法を含むデータ処理方法を指定する命令を組み込まれた暗号化対象データに対して、組み込まれた命令に従って暗号化処理を含むデータ処理を行うデータ暗号化方法であって、暗号化する範囲を指定する暗号化範囲指定命令が組み込まれた暗号化対象データに対して、前記暗号化範囲指定命令で指定された範囲を暗号化する手段を備える。

【0009】 また、前記暗号化対象データに、前記暗号化範囲指定命令に加え、前記暗号化対象データの受信者を指定する受信者指定命令が組み込まれている場合には、前記受信者指定命令で指定された受信者が保持する復号鍵に対応する暗号化鍵を用いて、前記暗号化対象データのうちの、前記暗号化範囲指定命令により指定された範囲を暗号化する手段を備える。

【0010】 また、前記暗号化対象データを暗号化するに際し、前記暗号化対象データを第1の暗号化鍵で暗号化し、前記第1の暗号化鍵に対応する第1の復号鍵を、受信者の保持する第2の復号鍵に対応する第2の暗号化鍵で暗号化し、暗号化された前記暗号化対象データに、暗号化された前記第1の復号鍵を指定する復号範囲指定命令を組み込んだ暗号化データを得る手段を備える。

【0011】 また、復号処理方法を含むデータ処理方法を指定する命令を組み込まれた暗号化データに対して、組み込まれた命令に従って復号処理を含むデータ処理を行なうデータ暗号化方法であって、復号する範囲を指定する復号範囲指定命令が組み込まれた暗号化データに対して、前記復号範囲指定命令で指定された範囲を復号する

するネットワーク3と、暗号化対象データ生成装置4と、ユーザ生成装置5によって構成される。

[0029] データ送信装置1は、データ受信装置2からのデータ要求情報及びオプショナルとして受信者識別情報を受信しそのデータ要求情報に対応した暗号化データをデータ受信装置2に送信するためのデータ通信手段11と、上記データ要求情報に対応する暗号化対象データをデータ送信手段13から取り出し、この暗号化対象データをデータ送信手段14に渡し、その結果として生成される暗号化データを取得し、この暗号化データをデータ通信手段に渡すためのデータ取得手段12と、暗号化対象データを保管するデータ保管手段13と、暗号化対象データを受信者識別情報もしくは後で述べる受信者指定命令にて指定された受信者向けに暗号化して暗号化データを生成するためのデータ暗号化手段14を備えている。データ暗号化手段14は、図示していないがユーザ生成装置5によって生成された各ユーザのユーザ公開鍵を保管するための公開鍵保管手段を備えている。データ暗号化手段14の詳細構成については後で説明する。

[0030] データ送信装置1としては、具体的には、上記データ通信手段と、データ取得手段と、データ保管手段を備えた、既存のWWW(World Wide Web)サーバ(例えば、Netscape Communications社のNetscape Communicationサーバ)を実装したコンピュータ(パソコンやワークステーションなど)が利用できる。この場合、WWWサーバの備えるデータ通信手段11が、WWWサーバとWWWブラウザ間の標準通信プロトコルであるHTTPプロトコルに基づいてデータ通信を行う。

[0031] データ送信装置におけるデータ暗号化手段14の実現方法としては、具体的には、CGI(Common Gateway Interface)プログラム(各種データ処理機能をWWWサーバに追加するためのプログラム)を利用できる。データ送信装置1を、WWWサーバとCGIプログラムで実現する場合の構成図を図2(1)に示す。図2(1)に示すように、CGIプログラムを利用する場合は、データ送信装置は、データ暗号化手段を提供するCGIプログラム101が備えられたWWWサーバ100で構成され、CGIプログラム101とWWWサーバ100は一体のプログラムとして動作する。すなわち、CGIプログラムを利用する場合、WWWサーバ毎にCGIプログラムを追加する必要がある。

[0032] なお、データ送信装置におけるデータ暗号化手段14の別の実現方法として、暗号化処理代行プログラム(以下、暗号化プロセスと称する)を利用することもできる。暗号化プロセスで実現する場合のデータ送信装置の構成図を図2(2)に示す。

[0033] また、図3に、データ送信装置をWWWサーバと暗号化プロセスで構成した場合のシステムの全体構成を示す。

[0034] 図2(2)及び図3に示すように、暗号化

プロセスによる構成を利用する場合は、データ送信装置1は、WWWサーバ100と、データ暗号化手段14とデータ通信手段15を備えた暗号化プロセス102で構成される。

[0035] ここで暗号化プロセス102におけるデータ通信手段15は、WWWサーバとWWWブラウザ間のデータの通信のための標準プロトコルであるHTTPプロトコルに基づいてデータ通信を行う。

[0036] この構成により、WWWサーバ100と暗号化プロセス102は、それぞれ独立のプログラムとして動作させることが可能となる。そして、その結果、WWWサーバによって既存のWWWサーバへの暗号化プロセスでデータ暗号化手段を追加することも可能となる。

[0037] また、データ受信装置2は、データ送信装置1にデータ要求情報及びオプショナルとして受信者識別情報を送信し、そのデータ要求情報に対応した暗号化データを受信するためのデータ通信手段21と、受信した暗号化データをデータ復号手段23とし、その結果として得られる復号された暗号化データに対して、各種データ処理(例えばデータの表示、データの保存、データの印刷などの処理)を施すためのデータ処理手段22と、暗号化データを復号して、復号された暗号化データを生成するためのデータ復号手段23と、ユーザから各種データの処理の指定(例えば取得したいデータの指定、データの保存やデータの印刷などの処理の指定など)を受けるためのデータ入力手段23と、データの表示やデータの印刷などのためにディスプレイやプリンタなどの外部装置にデータを出力するためのデータ出力手段24を備えている。

[0038] データ復号手段23は、図示していないが復号生成装置5によって生成されたユーザ秘密鍵(このデータ受信装置を利用するユーザのユーザ秘密鍵)を保管するための公開鍵保管手段を備えている。データ復号手段25の詳細構成については後で説明する。

[0039] データ受信装置2としては、具体的には、上記データ通信手段と、データ処理手段を備えた既存のWWWブラウザ(例えば、Netscape Communications社のNetscape Navigatorや、Microsoft社のInternet Explorer)を実装したコンピュータ(パソコンやワークステーションなど)が利用できる。この場合、WWWブラウザの備えるデータ通信手段21が、WWWサーバとWWWブラウザ間の標準通信プロトコルであるHTTPプロトコルに基づいてデータ通信を行う。また、データ入力手段としては、上記コンピュータの備えるキーボードやマウス等を利用できる。またデータ出力手段にはディスプレイやプリンタ等が接続されている。

[0040] データ受信装置2におけるデータ復号手段25の実現方法としては、具体的には、WWWブラウザのブラウザイン(各種データ処理機能をWWWブラウザに追加

するためのプログラム)を利用することができ、データ復号手段を、ブラウザ上で実現する場合のデータ復号手段の構成図を図2(3)に示す。図2(3)に示すように、ブラウザインを利用する場合は、データ受信装置は、データ復号手段を提供する復号ブラウザイン201が組み込まれたWWWブラウザ200で構成され、WWWブラウザと復号ブラウザインは一体のプログラムとして動作する。

[0041] すなわち、ブラウザインを利用する場合、WWWブラウザ毎にブラウザインを追加する必要がある。

[0042] なお、データ受信装置におけるデータ復号手段14の別の実現方法として、復号処理代行プログラム(以下、復号プロセスと称する)を利用することもできる。復号プロセスで実現する場合のデータ受信装置の構成図を図2(4)に示す。また、図3に、データ受信装置をWWWブラウザと復号プロセスで構成した場合のシステムの全体構成を示す。

[0043] 図2(4)及び図3に示すように、復号プロセスによる構成を採用する場合は、データ受信装置2は、WWWブラウザ200と、データ復号手段23に加えデータ通信手段21を備えた復号プロセス202で構成される。

[0044] ここで復号プロセス202におけるデータ通信手段は、WWWサーバとWWWブラウザ間のデータ通信のための標準プロトコルであるHTTPプロトコルに基づいてデータ通信を行う。

[0045] この構成により、WWWブラウザ200と復号プロセス202は、それぞれ独立のプログラムとして動作させることが可能となる。そして、その結果、WWWブラウザによって既存のWWWブラウザがそのまゝ利用でき、また、複数のWWWブラウザに一つの復号プロセスでデータ復号手段を追加することも可能となる。

[0046] 暗号化対象データ作成装置4としては、暗号化対象データを作成する暗号化対象データ作成手段41と、作成した暗号化対象データをデータ送信手段1のデータ保管手段13に配送するデータ配送手段42が備えられている。

[0047] 暗号化対象データ作成装置4として、具体的には、通常のテキストエディタや既存のWWWブラウザ(ホームページなど)を作成するための市販のソフトウェアが実装されたコンピュータ(パソコンやワークステーション)が利用できる。またデータ配送手段42の具体的な実現方法としては、例えば、暗号化対象データをフロッピーディスクなどの記録媒体に記録してケーブルで配送する手段をとることができる。

[0048] 暗号化対象データのデータ構造については、後で説明する。ユーザ生成装置5は、各ユーザ毎に固有のユーザ秘密鍵及びユーザ公開鍵を生成するユーザ生成手段51と、生成したユーザ秘密鍵をデータ受信装置の公開鍵保管手段に配送するとともに、生成した

ユーザ公開鍵を、データ暗号化装置の公開鍵保管手段に配送するためのユーザ鍵配送手段52を備えている。ユーザ生成装置5としては、具体的には、ユーザ鍵生成プログラムを実装したパソコンやワークステーションなどを利用できる。またユーザ秘密鍵を配送するためのユーザ鍵配送手段としては、例えば、ICカードなどの物理的に安全な媒体に記録してオンラインで配送する手段や、ユーザ秘密鍵をユーザのパスワード等を用いて共通鍵暗号方式により暗号化した上でフロッピーディスク等の記録媒体に記録して配送する手段や、パソコン等で暗号化されたユーザ秘密鍵をネットワークを利用して配送する手段などを利用することができ、また、ユーザ公開鍵を配送するためのユーザ鍵配送手段としては、例えば、ICカードなどの物理的に安全な媒体に記録して配送する手段や、認証局と呼ばれる公的機関にユーザ公開鍵に対する証明書の発行を受けた上で、ユーザ公開鍵と証明書とをフロッピーディスクなどの記録媒体に記録してオンラインで配送する手段や、または、ユーザ公開鍵と証明書をネットワークを利用してオンラインで電子的に配送する手段などを利用することができ、

[0049] なお、ここでは、データ送信装置1、データ受信装置2、暗号化対象データ作成装置4、ユーザ生成装置5は、それぞれ異なる装置として実現する場合について説明したが、これらの装置を同じコンピュータで実現することも可能である。例えば、ユーザ利用するコンピュータに、暗号化対象データ作成装置と、データ受信装置と、ユーザ鍵生成装置の各機能を付した構成も可能である。

[0050] 「暗号化対象データ及び暗号化データの構造」次に、本発明の形態で扱う、暗号処理を含むデータ処理命令が組み込まれた暗号化対象データと、この暗号化対象データを組み込んだ命令に就いて暗号化した結果として得られる暗号化データのデータ構造について説明する。

[0051] なお、ここでは、暗号化対象データおよび暗号化データとして、WWWデータの標準的な記述言語である、HTML(Hypertext Markup Language)言語に基づいて作成する場合について説明するが、他の記述言語に基づいて作成する場合についても可能である。

[0052] 図5(1)は、本発明の形態で扱う暗号化対象データの構造例である。図5(1)に示すように、暗号化対象データD1は、通常のHTML言語で記述されたデータ本体D10に、暗号化するデータ範囲を指定する暗号化範囲指定命令C1や、この暗号化対象データの受信者を指定する受信者指定命令などの暗号処理命令が追加された構造となる。

[0053] また、図5(2)は、本発明の形態で扱う暗号化データの構造例である。図5(2)に示すように、暗号化データD2は、復号する範囲を指定する復号範囲指定命令C2や、この暗号化データの受信者が復号す

【0054】図6に、暗号対象データ及び暗号化データ

【10055】また、受信者指定命令は、必要に応じて指

【0056】データ提供者は、受償者指定命令を利用す

【10057】また、暗号化範囲指定命令は、具体的に

この命令をコメント命令と称する)。したがって、既存

ように他の町号処理命令も、HTML言語のコメント命令を

【0058】「データ暗号化手段及びデータ復号手段の

【0059】まず、データ町号化手段14の詳細構成を

【0060】データ復号手段13の詳細構成を図4

のふたは、東京新聞社が、これを非道徳行為と

手段において利用したものと同一公開鍵暗号方式を用い

【0061】「詳細な動作」次に、本実施の形態の動作

【0063】(1) 本実施の形態全体の動作概略

【0064】図7に示すように、本実施の形態は、新規

【0065】ここでユーザ鍵生成処理(S100)は、

【0066】データ作成処理(S200)は、データ読

【0067】データ取得処理（S300）は、各ユーザ

【0068】(2) ユーザ生成処理 (S100) の

【0069】図8に示すように、ユーザ鍵生成処理で

段に配送し（ステップS120）、データ受信装置にお

【0070】ユーザ秘密鍵が第三者に露見しないように

配送するか、または、ICカードを利用して手渡しで配送

【0071】(3) データ作成処理(S200)の詳細

【0072】図9に示すように、データ作成処理では、

【0073】暗号化対象データを配送するための具体的な

【0074】(4) データ取得処理(S300)の詳

【0075】図10に示すように、データ取得処理で

データ送信装置のWWWサーバにおいて、データ通信手段に

0)、データ通信手段により、暗号化データをデータ受

段により、複写された暗号化データを、タイムシフト

【0076】ここで、ステップS310においてユーザ

【0077】また、図11(1)は、データ暗号化手段

(ステップS351)、共通暗号化手段により、生成したデータを用いて、暗号化対象データの暗号化範囲指定命令で指定された範囲を暗号化し(ステップS352)、公開鍵暗号化手段により、ユーザ公開鍵暗号化手段に宛てられている各ユーザのユーザ公開鍵の中から、受信者指定命令、もしくは、受信者識別情報で指定された受信者のユーザ公開鍵を取得し、取得したユーザ公開鍵を利用して、公開鍵暗号化し(ステップS353)、暗号化データ作成手段により、暗号化されたデータを指定する暗号範囲指定命令と復号範囲指定命令を組み込んだ暗号化データを作成する(ステップS354)。

【0079】また、図11(2)は、データ復号手段における暗号化データの復号(ステップS380)の詳細な動作を示すフローチャートである。

【0080】図11(2)に示すように、データ復号手段では、暗号化データ解析手段により、暗号化データから復号範囲指定命令で指定された暗号化されたデータを取得し(ステップS381)、公開鍵暗号化手段により、ユーザ秘密鍵保管手段に保管されたユーザ秘密鍵を用いて、暗号化されたデータを復号し(ステップS382)、共通復号手段により、復号されたデータ復号手段を用いて暗号化データを復号し(ステップS383)、復号された暗号化データを取得する(ステップS384)。

【0081】なお、暗号化対象データに受信者指定命令を組み込むことにより、暗号化対象データの受信者を指定する場合は、データ受信装置からデータ送信装置に受信者識別情報を送信する必要がある。

【0082】次に、データ送信装置を、WLANサーバと暗号化デバイスで、データ受信装置を、WLANサーバと復号プロセッサで構成する場合の詳細動作について説明する。図12は、この場合のデータ取得処理の詳細動作を示すフローチャートである。

【0083】図12に示すように、データ取得処理では、まず、データ受信装置のWLANサーバにおいて、ユーザ入力手段により、ユーザから取得したいデータの指定を受け取り(ステップS410)、データ通信手段により、指定されたデータの送信を要求するデータ要求情報と、アドレスとして受信者を指定する受信者識別情報と、データ送信装置に送信し(ステップS420)、データ送信装置のWLANサーバにおいて、データ通信手段により、データ要求情報と受信者識別情報を受信し(ステップS430)、データ取得手段により、受信したデータ要求情報に対応する暗号化対象データを取得し(ステップS440)、データ通信手段により暗号化対象データを暗号化プロセッサに送信し(ステップS450)、暗号化プロセッサにおいて、データ通信手段により暗号化対象データを受信し(ステップS460)、データ暗号化手段により、取得された暗号化対象データを、受信者

指定命令、もしくは、受信者識別情報で指定された受信者のみで復号できるように暗号化して、暗号化データを生成し(ステップS470)、データ通信手段により、暗号化データを復号プロセッサに送信し(ステップS480)、データ送信装置の復号プロセッサにおいて、データ通信手段により、暗号化データを受信し(ステップS490)、データ復号手段により、暗号化データを復号し(ステップS500)、データ通信手段において、復号された暗号化データをWLANサーバに送信し(ステップS510)、WLANサーバのデータ通信手段により、復号された暗号データを受信し(ステップS520)、データ復号手段により、復号された暗号化データを、デバイス表示などのためにデータ出力手段に渡す(ステップS530)。

【0084】(実施の形態2) 次に、データ送信装置にあらかじめ暗号化データを格納しておき、データ送信装置にて、データ受信装置からの送信要求に対応して、該当の暗号化データをデータ受信装置に送信し、データ受信装置にて、受信した暗号化データを復号して取得する場合について説明する。

【0085】まず、システム構成について説明し、次に、本システムの詳細な動作について説明する。

【0086】システムの構成、本実施の形態の全体のシステム構成について説明する。図13は、本実施の形態におけるデータ暗号通信システムの概略構成図である。図13に示すようにデータ暗号通信システムは、データ送信装置1と、データ受信装置2と、これらを接続するネットワーク3と、暗号化データ作成装置6と、ユーザ復号装置5とによって構成される。

【0087】ここで、データ受信装置1及び、ユーザ復号装置2の構成は、実施の形態1と同じものが利用できるので、ここでは説明を省略する。

【0088】データ送信装置1は、データ受信装置2からのデータ要求情報及びアドレスとして受信者識別情報を受信し、そのデータ要求情報に対応した暗号化データをデータ送信装置2に送信するためのデータ通信手段1と、上記データ要求情報に対応する暗号化データをデータ復号手段13から取り出し、この暗号化データをデータ通信手段に渡すためのデータ取得手段12と、暗号化データを保管するためのデータ保管手段13で構成される。

【0089】データ送信装置1としては、具体的には、上記データ通信手段と、データ取得手段と、データ保管手段とを備え、既存のWLAN(Wireless Local Area Network)サーバ(例えば、Access CommunicationのAccess Communicationサーバ)と接続したコンピュータ(パーソナルコンピュータ)を利用できる。この場合、WLANサーバの備えるデータ通信手段11が、WLANサーバとWLANサーバ間の無線通信プロトコルであるHTTPプロトコルに基づいてデータ通信を行う。

【0090】暗号化データ作成装置6としては、暗号化対象データを作成する暗号化対象データ作成手段61と、作成した暗号化対象データを暗号化対象データを受信者指定命令にて指定された受信者向けに暗号化して暗号化データを生成するためのデータ暗号化手段62と、暗号化データをデータ送信装置のデータ保管手段13に配送するデータ配送手段63を備えている。データ暗号化手段には、図示していないが暗号化手段5によって生成された各ユーザのユーザ公開鍵を保持するための公開鍵管理手段を備えている。データ暗号化手段14の詳細構成については実施の形態1の場合と同じであるので説明を省略する。

【0091】暗号化データ作成装置として、具体的には、通常のデキストトップエディタや既存のWLANサーバ、及び、データ暗号化手段を実現するプログラムとが実装されたコンピュータ(パーソナルコンピュータ)が利用される。

【0092】またデータ配送手段42の具体的な実現方法としては、例えば、暗号化対象データをフローティングディスクなどの記憶媒体に記録してネットワークに配送する手段等とすることができ。

【0093】暗号化対象データ及び暗号化データのデータ暗号化については、実施の形態1の場合と同じであるので説明を省略する。

【0094】「詳細な動作」次に、本実施の形態の動作について説明する。

【0095】まず、全体の動作概略について説明し、その後、個々の処理の詳細動作について説明する。

【0096】(1) 本実施の形態全体の動作概略 本実施の形態におけるデータ暗号通信システムの全体の動作概略としては、実施の形態1と同様であり、新規のユーザが利用を開始するときに行うユーザ復号装置(ステップS100)と、データの提供者が提供データ(暗号化データ)を作成するときに行う暗号化データ作成装置(ステップS200)と、ユーザが、提供データを取得するときに行うデータ取得装置(ステップS300)からなる。

【0097】ここでユーザ復号装置(S100)は、実施の形態1と同様に、ユーザ自身、もしくは、本システムの管理者が、ユーザ復号装置を利用して行う。具体的には、各ユーザ用のユーザ秘密鍵と、ユーザ復号装置に対応するユーザ公開鍵を生成し、生成したユーザ秘密鍵をそのユーザが利用するデータ受信装置に、またユーザ公開鍵を、データ送信装置に配送するなどの処理を行う。

【0098】データ作成装置(S200)は、実施の形態1と異なり、データ提供者が、暗号化データ作成装置を利用して行う。

【0099】具体的には、暗号化対象データを作成し、

作成した暗号化対象データを暗号化し、データ送信装置に配送するなどの処理を行う。

【0100】データ取得装置(S300)は、実施の形態1と異なり、各ユーザが、データ受信装置を利用して行う。具体的には、各ユーザが、自分のデータ受信装置を利用して、取得したい提供データ(暗号化データ)の送信を要求するデータ要求情報とデータ送信装置に送信し、データ送信装置から、そのデータ要求情報に対応する暗号化データを受信し、受信した暗号化データを復号し、取り出すなどの処理を行う。

【0101】(2) ユーザ復号装置(S100)の詳細動作

ユーザ復号装置の動作は、実施の形態1の場合と同じであるので説明は省略する。

【0102】(3) データ作成装置(S200)の詳細動作

図14は、データ作成装置の詳細動作を示すフローチャートである。

【0103】図14に示すように、データ作成装置では、暗号化データ作成装置において、暗号化対象データ作成手段により、暗号化範囲指定命令と受信者指定命令などを含む暗号化対象データを作成し(ステップ210)、暗号化対象データを、受信者指定命令で指定された受信者のみで復号できるように暗号化して、暗号化データを作成し(ステップ220)、データ配送手段により、作成した暗号化対象データを、データ送信装置のデータ保管手段に配送し(ステップ230)、データ送信装置において、暗号化データを保管する(ステップ240)。

【0104】データ暗号化手段における暗号化対象データの暗号化(ステップS220)の詳細な動作は実施の形態1の場合と同様であるので説明は省略する。

【0105】暗号化データを配送するための具体的な実現方法としては、暗号化データをフローティングディスクなどの記憶媒体に記録して手渡しで配送する方法や、ネットワークを利用してオンラインで配送するなどの手段が利用される。

【0106】(4) データ取得装置(S300)の詳細動作

まず、データ受信装置を、WLANサーバと復号プロセッサで構成する場合の詳細動作について説明する。図15は、この場合のデータ取得装置の詳細動作を示すフローチャートである。

【0107】図15に示すように、データ取得装置では、まず、データ受信装置のWLANサーバにおいて、ユーザ入力手段により、ユーザから取得したいデータの指定を受け取り(ステップS310)、データ通信手段により、指定されたデータの送信を要求するデータ要求情報と送信し(ステップS320)、データ送信装置のWLANサーバにおいて、データ通信手段により、データ要求

情報と受信者識別情報を受信し（ステップS330）、データ取得手段により、受信したデータ要求情報に対応する暗号化データを取得し（ステップS340）、データ通信手段により、暗号化データをデータ受信装置に送信し（ステップS350）、データ受信装置において、データ通信手段により、暗号化データを受信し（ステップS360）、データ復号手段により、暗号化データを復号し（ステップS370）、データ処理手段により、復号された暗号化データを、ディスプレイ表示とのためデータ出力手段に渡す（ステップS380）。

【0108】データ復号手段における暗号化データの復号（ステップS370）の詳細な動作は実施形態1の場合と同様であるので説明は省略する。

【0109】次に、データ受信装置を、データ復号手段と復号プロキシで構成する場合の詳細動作について説明する。図16は、この場合のデータ取得処理の詳細動作を示すフローチャートである。

【0110】図16に示すように、データ取得処理では、まず、データ受信装置のデータ復号手段において、ユーザ入力手段により、ユーザから取得したいデータの指定を受け取り（ステップS410）、データ通信手段により、指定されたデータの送信を要求するデータ要求情報、データ送信装置に送信し（ステップS420）、データ送信装置のデータ復号手段において、データ復号手段により、データ要求情報と受信者識別情報を受信し（ステップS430）、データ取得手段により、受信したデータ要求情報に対応する暗号化データを取得し（ステップS440）、データ通信手段により、暗号化データを復号プロキシに送信し（ステップS450）、データ受信装置の復号プロキシにおいて、データ通信手段により、暗号化データを受信し（ステップS460）、データ復号手段により、暗号化データを復号し（ステップS470）、データ通信手段において、復号された暗号化データをデータ復号手段に渡す（ステップS480）、データ復号手段により、復号された暗号化データを受信し（ステップS490）、データ復号手段により、復号された暗号化データを、ディスプレイ表示とのためデータ出力手段に渡す（ステップS500）。

【0111】なお、実施形態1及び、実施形態2では、データの送信及びデータの受信は、データ受信装置及びデータ送信装置において説明したがそれに限るものではない。

【0112】また、データとして、HDL言語に基づいて各データ処理の命令を組み立てたデータの場合について説明したが、それに限るものではない。

【0113】また、データの暗号化手段として、データの暗号化に共通暗号方式を利用し、データの暗号化に利用したデータの暗号化に公開暗号方式を利用する場合について説明したが、それに限るものではない。

【発明の効果】本発明によれば、暗号化対象データに、暗号化する処理を指定する暗号化範囲指定命令を組み込むことにより、暗号化対象データは、暗号化範囲指定命令で指定された範囲のみ暗号化される。このため、必要に応じて、暗号化対象データの重要な部分のみを暗号化したり、一部はすべての受信者に視認させることが可能となる。

【0115】また、暗号化対象データに、受信者を指定する受信者指定命令を組み込むことにより、暗号化対象データを、指定した受信者以外には復号できないように暗号化することが可能となる。すなわち、必要に応じて、あらかじめ受信者を指定することが可能となる。

【0116】また、特に、データ送信装置を、データサーバと、暗号化対象データの暗号化範囲指定命令で指定された範囲のみを暗号化するためのデータ暗号化手段とデータ復号手段及びデータ復号手段との間でデータの送受信を行うためのデータ通信手段とを備えた暗号化プログラムとを接続したコンピュータで構成することにより、既存のデータサーバを変更することなく利用した、データの暗号化を行うデータ暗号化装置が提供可能となる。

【0117】同様に、特に、データ復号装置を、データサーバと、暗号化データの暗号化範囲指定命令で指定された範囲のみを復号するデータ復号手段とデータ復号手段とを備えた復号プログラムとを、接続したコンピュータで構成することにより、既存のデータサーバを変更することなく利用した、暗号化データの復号受信を行うデータ暗号化装置が提供可能となる。

【0118】また、特に、HDL言語のコメント命令を利用して暗号化命令を定義するため、既存のデータサーバやプログラムに影響を与えることがない。

【図面の簡単な説明】

【図1】 本発明の実施形態1のデータ暗号通信システムの全体構成図

【図2】 データ送信装置及びデータ受信装置の構成図

【図3】 暗号化プロキシ及び復号プロキシを利用したデータ暗号通信システムの全体構成図

【図4】 データ暗号化手段及びデータ復号手段の詳細構成図

【図5】 暗号化対象データ及び暗号化データのデータ構造例を示す図

【図6】 暗号化命令の一覧を示す図

【図7】 全体の動作概要を示すフローチャート

【図8】 ユーザ生成暗号処理のフローチャート

【図9】 データ作成処理のフローチャート

【図10】 データ取得処理のフローチャート

【図11】 データ暗号化手段及びデータ復号手段の処理のフローチャート

【図12】 暗号化プロキシ及び復号プロキシ利用時のデータ取得処理のフローチャート

【図1】 本発明の実施形態1のデータ暗号通信システムの全体構成図

【図14】 データ作成処理のフローチャート

【図15】 データ取得処理のフローチャート

【図16】 復号プロキシ利用時のデータ取得処理のフローチャート

【符号の説明】

1 データ送信装置

2 データ受信装置

4 暗号化対象データ作成装置

5 ユーザ生成装置

14 データ暗号化手段

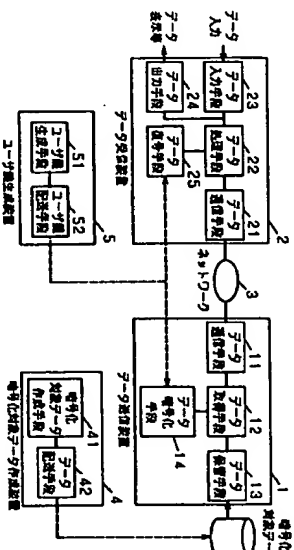
25 データ復号手段

101 暗号化プロキシ

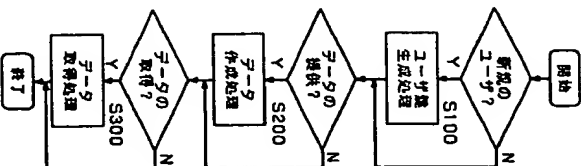
200 データサーバ

201 復号プロキシ

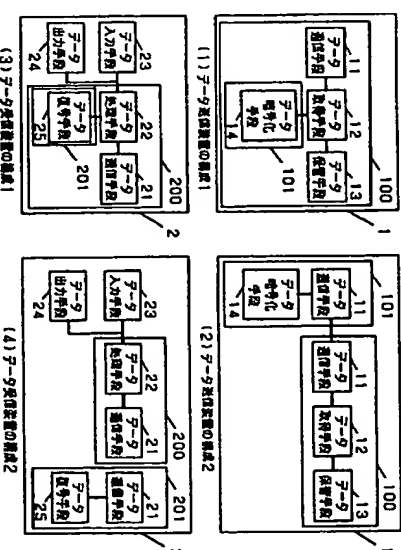
【図1】



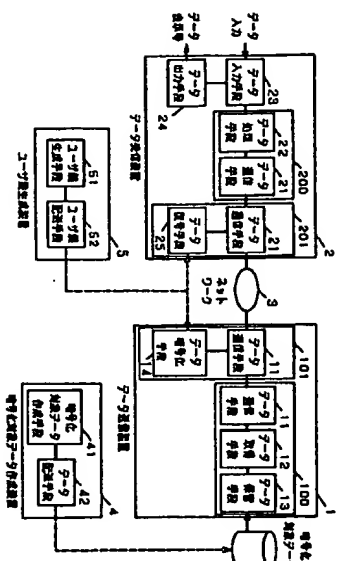
【図7】



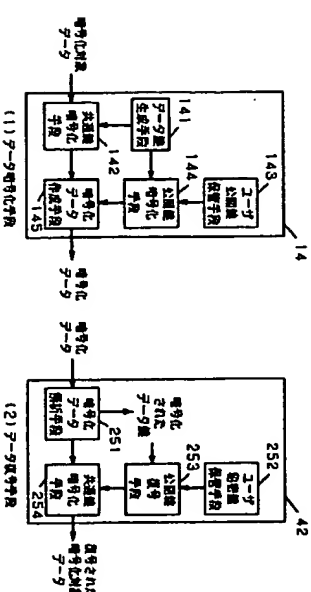
【図2】



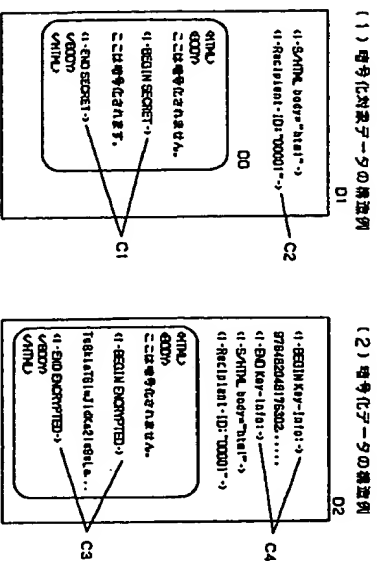
【図3】



【図4】



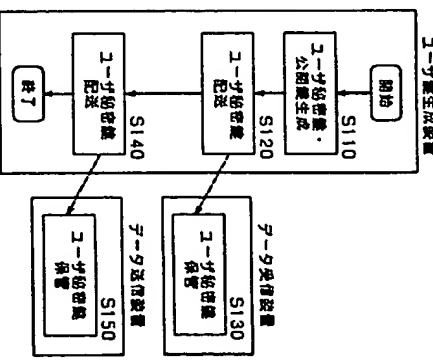
【図5】



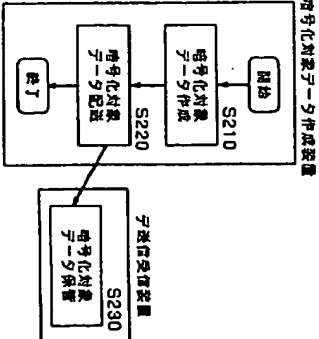
【図6】

命令	指定方法
暗号化 範囲指定命令	暗号化する範囲の開始を 「BEGIN SECRET」で指定し 終了を「END SECRET」 で指定する
受信命令 指定命令	受信データの暗号番号を以下のように 指定する 「-Recipient-ID: 10001」
復号化範囲 指定命令	復号する範囲の開始を 「BEGIN ENCRYPTED」で指定し 終了を「END ENCRYPTED」 で指定する
暗号情報 指定命令	暗号情報を以下のように指定する。 「-EO Key: 10101」

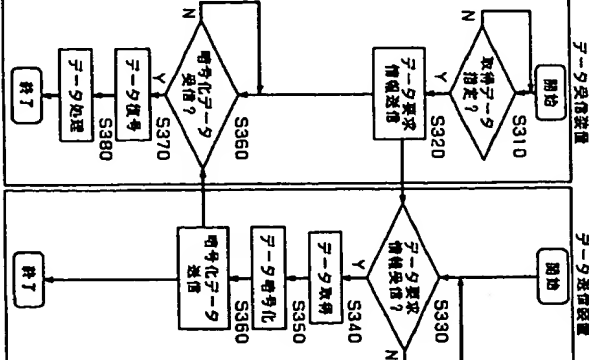
【図8】



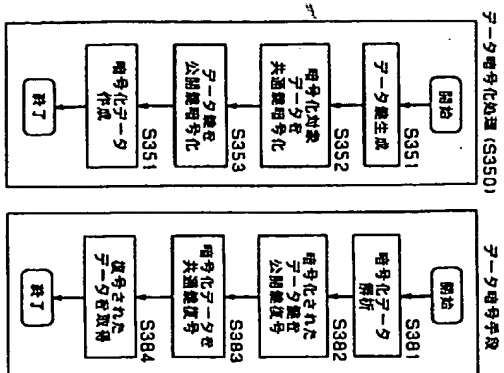
【図9】



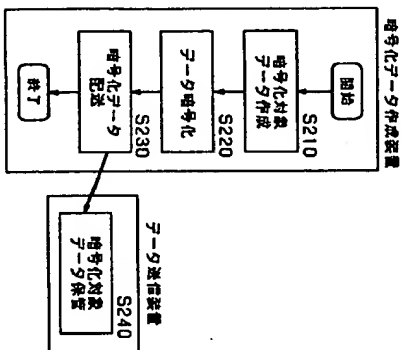
【図10】



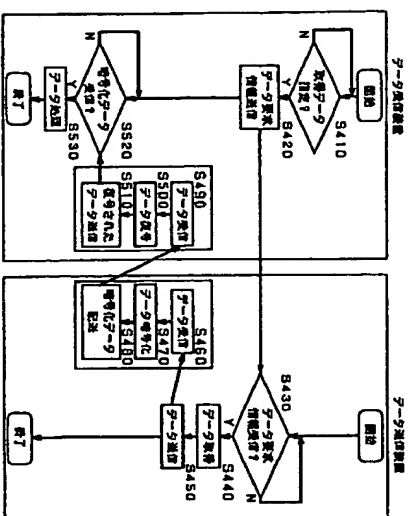
【図11】



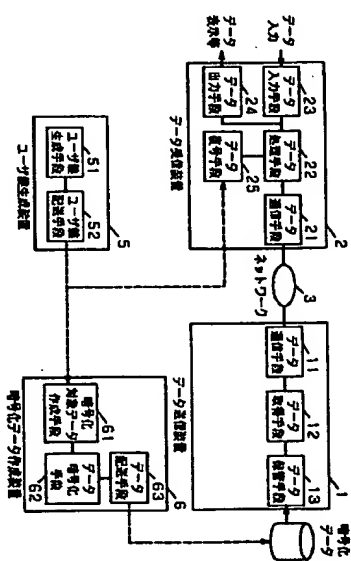
【図14】



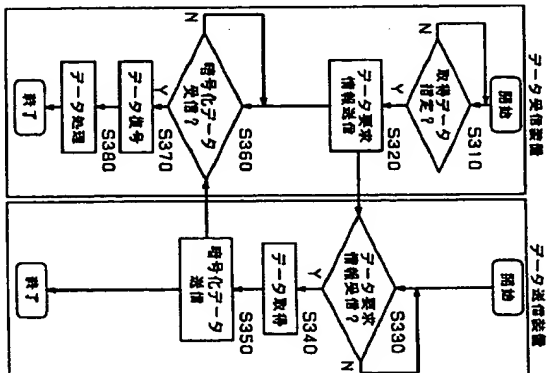
【図12】



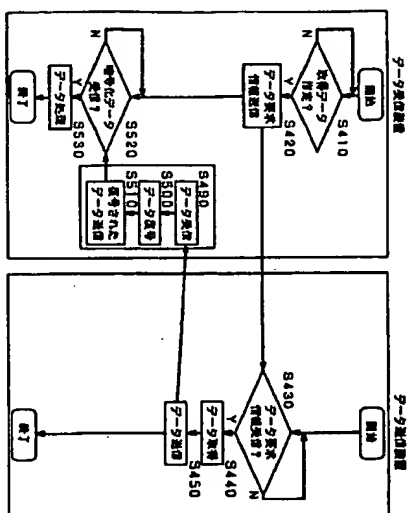
【図13】



【図15】



【図16】



フロントページの続き

(72)発明者 西條 盛
愛知県名古屋市中区栄2丁目6番1号白川
ビル別館5階 株式会社松下電器情報システム名古屋研究所内

(72)発明者 小野 貴敏
愛知県名古屋市中区栄2丁目6番1号白川
ビル別館5階 株式会社松下電器情報システム名古屋研究所内